



Virtualisation & Security Considerations

Virtualisation technology is not new; it has been around for at least 10 years, mainly in labs and development environments. However, it is now increasingly being used in production environments and all of the usual suspects – IBM, SUN, HP, Microsoft etc. - are investing heavily in beefing up their offerings in this space, either through acquisition or internal development. As the take up of virtualisation technology increases, questions are being asked about the security implications associated with its use. This article sets out to address those questions.

Dual Perspectives

When looking at security issues in the field of virtualisation, there are two perspectives. On the one hand there is the question of what security issues are associated with the take up of virtualisation within an organisation (particularly when it is used in a production environment). On the other hand there is the question of how virtualisation technology can be used to support improved security processes, particularly in the fields of disaster recovery, ensuring ongoing availability of critical systems, and patch management.

Security Issues With Virtualisation

First we will explore what security issues are associated with the take up of virtualisation within an organisation.

Like any other system, virtual machines will require to be secured and updated with the security updates that the vendor releases. Depending on the role of the virtual machine you may be required to perform additional hardening and implementation of antivirus and intrusion prevention systems. In brief a virtual machine will require the same security practices as the rest of the physical environment.

The host of a virtual machine carries extra significance given that if it is insecure, multiple virtual machines could be affected due to the fact the virtual machines and the host have established communication paths.

System Sense
Level 3, 1 James Place
North Sydney, NSW 2060



Phone: 99226136
Fax: 99224257
E-mail: info@systemsense.com.au
Web: www.systemsense.com.au



For example if a malicious user manages to detect and take control of a virtual machine they may be able to take control of the host and then all the other virtual machines associated with that host.

The following steps are recommended to mitigate the security risks associated with a virtual machine set up:

1. It is essential that the host is fully hardened with all settings being specifically addressed (rather than just relying on the default "out of the box settings" for that server model).
2. Proper security of each of the virtual machines needs to be applied by following a security hardening procedure, tools and policies.
3. Patching of the virtual machines and - most importantly - for the virtual host software.
4. Use of network segmentation between the virtual machines, especially if they have DMZ facing roles. The use of the software VLAN through the host software is not advised as it carries the same risks with the use of VLAN in the physical networks.
5. Additionally further restricting the access of the virtual host management console to the administration management subnets only will minimize the risk that a malicious user could access the console.
6. The general policy of a very secure password or pass phrases for the access of the console of the virtual host.
7. The use of security domain between the virtual machines to ensure that even when the machines are located on the same virtual host, they are still segmented according to their business function. Especially when machines are DMZ facing, dedicated network cards are required and relevant fire-wall configuration that restricts access to the specific adapter.
8. Also for DMZ facing virtual machines it is a good idea to limit the interoperability with the virtual

System Sense
Level 3, 1 James Place
North Sydney, NSW 2060



Phone: 99226136
Fax: 99224257
E-mail: info@systemsense.com.au
Web: www.systemsense.com.au



The most advanced configurations of the ESX Server from VMWare will ensure LUN segmentation and security. Specifically, each virtual machine sees only the virtual disks that have been presented to its virtual SCSI adapters. Virtual machines cannot see the physical Fibre Channel HBAs on the ESX Server host on which they run, nor, in typical use cases, do they see the LUNs on which their virtual disks reside.

Emerging mechanisms for LUN security in a virtual environment from Fibre Channel HBA vendors provide an alternative for accomplishing the same goals. In a physical Fibre Channel SAN environment, LUN security is typically accomplished through a combination of LUN masking and zoning. Using these approaches in a vendor-recommended way ensures that a given LUN can be accessed only by a single host, as identified by the world wide names (WWN) of its HBAs. Virtual machines can see and access only specific units of storage that the ESX Server administrator explicitly allows. This applies whether the virtual machine is using virtual disks on a VMFS file system or raw device mappings. The operating system within the virtual machine cannot change its own storage access nor interrogate a unit of storage in a way that allows it to discover any other storage units not defined by the ESX Server administrator.

Using Virtualisation To Enhance Security

Every production environment has several servers that are required as part of the core networking services. These servers may run DNS, DHCP, Radius, File and Print Services and Domain Controllers for Microsoft Active Directory implementations. From our experience monitoring core servers, we find that on average these servers are usually running only 5 to 10% of the available processor utilisation and 0.5GB of memory. Virtualisation can be used as a way to better utilise the server hardware by centralising such functions into virtual machines.

Currently, availability SLA's of production environments' are reported to be approx 99,99 %. Realistically, this represents a maximum downtime of 2-3 hours per month. Some specific services, such as e-mail and remote access have evolved to the point where they are required to be available 24x7.

System Sense
Level 3, 1 James Place
North Sydney, NSW 2060



Phone: 99226136
Fax: 99224257
E-mail: info@systemsense.com.au
Web: www.systemsense.com.au



The only way to deliver such high availability and service requirements is by building infrastructure that is redundant and has no single point of failure. Often the investment for such infrastructure can be significant and virtualisation offers the benefit of providing a flexible type of redundancy without the excessive costs. For the example of having multiple physical servers for functions such as DNS, Radius or Proxy, you could consider making one server physical and keep a second one as virtual.

This type of deployment of virtualised servers can be easily incorporated into a Disaster Recovery or Business Continuity plan with the simplicity of powering up machines as required.

Another use of virtualisation to enhance security is to simulate complex production environments for the purposes of development and proof of concept, allowing testing over different operating systems as well as simulating front end and back end architectures. Deployment and validation of operating system updates and patches can be performed without impacting production systems.

Virtual machines can also be used for stress testing of applications and to evaluate performance by varying the amount of memory and the number of processors assigned.

Finally in every technology refresh cycle you may have the requirement to perform migrations or configure complex inter-organisational identity solutions. Again virtualisation can be used to configure multiple active directory forest architecture, OS migrations and windows upgrades. The security advantage of performing the architectural changes and designs in a safe and contained environment is significant.

System Sense
Level 3, 1 James Place
North Sydney, NSW 2060



Phone: 99226136
Fax: 99224257
E-mail: info@systemsense.com.au
Web: www.systemsense.com.au